Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method for a secure transaction, comprising:

generating a first key from a user-supplied unencrypted password provided by a user computing device,

encrypting the user-supplied unencrypted password using the first key,

creating a user record, and

storing the encrypted password in the user record.

2. (Previously Presented) The computer-implemented method of claim 1, further comprising

upon user login, generating a second key from a would-be user's password using the same algorithm used to generate the first key from the user-supplied unencrypted password,

retrieving the corresponding user record,

decrypting the encrypted password in the user record using the second key, and

comparing the decrypted password with the would-be user-supplied password to see if they match.

3. (Previously Presented) The computer-implemented method of claim 2, further comprising

if the decrypted password and user-supplied password match, creating a temporary session record and storing the second key in the session record, otherwise aborting the user login.

4. (Previously Presented) The computer-implemented method of claim 3, further comprising

encrypting other sensitive user data using the first key and storing the encrypted data in the user record, and

during a session wherein a session record has been created, using the second key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.

5. (Previously Presented) The computer-implemented method of claim 1, further comprising

generating a public/private key pair,

storing the public key on an application server and the mating private key only on another server,

encrypting the original user-supplied unencrypted password with the public key and storing the public-key encrypted password on the application server, and

fetching the private key from the other server and using it to decrypt selected information on the application server.

6. (Previously Presented) The computer-implemented method of claim 5, wherein the other server is a secure off-site server.

7. (Currently Amended) A computer-executable program residing on a computer, the execution of the program causing the computer to:

generate a first key from user-supplied identification data provided by a user computing device,

encrypt the user-supplied identification data using the first key,

create a user record, and

store the encrypted identification data in the user record.

8. (Previously Presented) The computer-executable program of claim 7, further causing the computer to

upon user login, generate a second key from a would-be user's identification data supplied at login using the same algorithm used to generate the first key from the user-supplied unencrypted identification data,

retrieve the corresponding user record,

decrypt the encrypted identification data in the user record using the second key, and

compare the decrypted identification data with the would-be user-supplied identification data to see if they match.

9. (Previously Presented) The computer-executable program of claim 8, further causing the computer to

if the decrypted identification data and user-supplied identification data match, create a temporary session record and storing the second key in the session record, otherwise aborting the user login.

10. (Previously Presented) The computer-executable program of claim 9, further causing the computer to

encrypt other sensitive user data using the first key and storing the encrypted data in the user record, and

during a session wherein a session record has been created, use the second key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.

11. (Currently Amended) A computing device comprising:

a memory configured to store a first unencrypted password supplied from a user computing device; and

a processor configured to execute instructions to perform a method comprising:

generating a first key from the first user-supplied unencrypted password;

encrypting the first user-supplied unencrypted password using the first key;

storing the encrypted user-supplied password in a user record;

upon receiving a login request that includes a second unencrypted password from a would-be user, generating a second key from the second user-supplied unencrypted password in a manner equivalent to generating the first key from the first user-supplied unencrypted password;

using the second key to decrypt the first encrypted user-supplied password in the user record;

comparing the decrypted password and the second user-supplied unencrypted password to identify a match;

upon identifying a match, creating a temporary user session record and storing the second key in the temporary user session record.

12. (Previously Presented) The computing device of claim 11 further including:
encrypting sensitive user data using the first key;
storing the encrypted sensitive user data in the user record;
using the second key to decrypt the stored encrypted sensitive user data; and
storing the decrypted sensitive user data in the temporary user session record.